CLAIMS

1. A data storage device having a non-volatile memory for storing data content, and a control processor operable to evaluate selected said data content to establish whether there is a match between a characteristic of or a derivative of, said selected data content and a reference data content characteristic, or derivative, and to take an action in response to establishment of a said match.

2. A device according to claim 1 wherein said action includes sending information relating to an interaction between an accessing party and content accessed by said accessing party, said processor being adapted to send said information to a party that is not said accessing party.

3. A device according to claim 1 wherein said control processor is operable to perform at least one of:

(i) a sweep of data content stored in said memory in order to evaluate said content;

(ii) to perform an evaluation of content putatively to be added to said memory of the data storage device prior to said content being added to said memory.

4. A device according to claim 3 wherein said memory comprises file-serving memory and further including a content evaluating buffer memory for storing newly received content prior to or whilst newly received content is evaluated.

5. A device according to claim 3 wherein said memory comprises file-serving memory and further including a content evaluating buffer memory for storing newly received content prior to and whilst newly received content is evaluated.

6. A device according to claim 1 comprising a library of data content characteristics or derivatives.

7. A device according to claim 6 wherein said data content characteristics comprise an identity characteristic to identify said data content as being known, and wherein said identity characteristic is from the group:

(i) a signature derived from said data content;

(ii) a fingerprint derived from said data content.

8. A device according to claim 1 comprising a data content-related parameter correlation, said correlation linking content-related parameters with equivalent known data content characteristics or derivatives, said processor being adapted to use said parameters for determining said action.

9. A device according to claim 8 wherein said parameters are controllable by a third party.

10. A device according to claim 1 wherein said processor is configured to enable third party mediated control of said action.

11. A method of operating a network attached storage device, the method comprising

upon receipt of a request to store content, attempting to identify the content to be stored, and following a set of rules to be followed if the data content is identified or is not identified as being known, and

undertaking appropriate action in response to the identification of the identity of said data content to be stored in accordance with said set of rules.

12. A method according to claim 11 wherein said content comprises a data content entity from the list: file; database.

13. A method according to claim 12 wherein:

(i) a specific identity of a data content entity is identified; or;

(ii) a group or class of data content to which a particular data content belongs is identified.

14. A method according to claim 12 comprising streaming data content from a file.

15. A method according to claim 14 comprising streaming rich media data content.

16. A method according to claim 11 wherein said attempt to identify content of a data content entity comprises producing a signature or fingerprint using said data content and comparing said produced signature or fingerprint with reference signatures or fingerprints relating to data content whose identity is already known.

17. A method according to claim 11 wherein said appropriate action comprises performing an action from the group:

(i) storing said content;

(ii) not storing said content;

(iii) communicating with a third party;

(iv) informing a third party that said data content has been stored, or that an attempt to store it was made.

18. A method according to claim 11 further comprising interacting between a party external to the device that is not a data content accessing party accessing data content and the device.

19. A method according to claim 18 wherein said interaction comprises the external party performing at least one of:

(i) providing information into said device;

(ii) receiving information from said device.

20. A method according to claim 11 wherein there is third party mediated control of said appropriate action undertaken by said device to user requests to store and/or access data content.

21. A method according to claim 11 wherein there is a communication to said device of at least one of:

(i) a data content entity signature or fingerprint from a third party;

(ii) a parameter which interacts with said rules to assist in controlling what is said appropriate action.

22. A method according to claim 21 wherein said parameter comprises a cost of read access or of write access for a particular data content.

23. A method according to claim 11 comprising said data storage device ascertaining an identity of a computer device which has made a request to perform at least one of (a) store data content and (b) read data content.

24. A method according to claim 23 comprising providing an identity of an accessing party to an external party and/or providing to an external party information derived from that identity.

25. A method according to claim 11 wherein said appropriate action comprises generating or augmenting an account related to a user identity and/or an identity of said storage device, and wherein said account comprises at least one of:

(i) a financial account for request for payment;

(ii) an information account for analysis.

26. A method according to claim 11 performed on a device which has content-usage control parameters corresponding to and associated with each identified content, the method comprising using said content-usage parameters in determining what appropriate action is undertaken.

27. A method according to claim 26 performed with a device for enabling a third party to input said content-usage parameters to said device, said method comprising the third party inputting said content-usage parameters to said device.

28. A method according to claim 27 wherein said third party inputs at least one of:

(i) a price to be charged associated with said content;

(ii) a price to be charged to said device or an owner of said device;

(iii) a price to be charged to a party requesting storage of said content, or to an entity associated with the requesting party;

(iv) a limitation upon the use of said content.

29. A method according to claim 26 wherein a content rights owner maintains content-usage parameters accessible by said device at a location that is at least one of:

(i) off-device;

(ii) on-device.

30. A method according to claim 11 wherein said device is operable to interact with a party external to said device and said appropriate action comprises at least one of:

(i) communicating with a party external to said storage device;

(ii) providing information to a third party external to said device that is not the person requesting content to be stored;

(iii) issuing a request for payment to a party;

(iv) providing content-storage or use-related information to a rights owner who is recorded on said storage device as owning rights in content that has been identified;

(v) providing content-storage or use information to a third party that is not the owner of the rights to which the information relates.

31. A network attachable file server having:

a computer memory for storing files;

a file content monitor processor;

a reference library for file content related signatures and content-related attributes correlated with said signatures;

said processor being operable to evaluate content of a file for determining a content related attribute of the file and for acting in response to the evaluation of the content related attribute of the file;

the processor being operable to perform the evaluation by performing steps including obtaining from the library a signature or fingerprint of said file and comparing said obtained signature or fingerprint with stored signatures or fingerprints of said reference library for establishing a match, and for thereby establishing a correlated content-related attribute of said file, said processor being adapted to take said predetermined action dependent upon what content-related attribute of said file has been established.

32. A server according to claim 31 wherein said content-related attribute comprises at least one of:

(i) a unique file identity;

(ii) an identity of a class or kind of data content of said file.

33. A network having at least one Network Attached Storage Device, NASD, said NASD being arranged for performing the method of claim 1.

34. A network having at least one Network Attached Storage Device, NASD, said NASD including the server of claim 31.

35. A method of integrating storage of data files having a data content with management of rights associated with said data files using a network attached file server which is capable of accessing said data content of a file and which is capable of producing a report relating to at least one of (a) storage and (b) access of files having associated rights, the method comprising using said file server to assess files stored on it, or files to be stored on it, to determine if an attribute related to the

content of accessed files can be established by screening said content against known attributes, thus establishing said content as belonging to a known file or class of files, using the results of the assessment to produce said report.

36. The method of claim 35 further including transmitting said report externally of said file server.

37. A method according to claim 36 wherein said report comprises at least one of:

(i) a financial report used in the generation of an invoice;

(ii) market research information.

38. A machine readable data carrier storing a program which when run on a processor of a computer memory network attached storage device having a processor, a non-volatile memory, and a library of signatures or fingerprints, is adapted to cause said storage device to:

evaluate data content of a data content entity either stored in said memory or received by said device for storage in said memory and to create a signature or fingerprint derived from said data content and capable of identifying said data content;

and to compare said created signature or fingerprint with reference signatures or fingerprints held in said library of signatures or fingerprints for establishing whether said created signature or fingerprint matches a reference signature or fingerprint and for thereby establishing an identity of said data content; and

perform a predetermined act which is influenced by said identity of said data content.

39. The carrier according to claim 38 wherein said predetermined act includes communicating externally of said device information that is related to said identity of said data content.

40. The carrier according to claim 39 which causes said device to refer to a set of content-related parameters in determining what is to be said predetermined act.

41. The carrier according to claim 40 which is adapted to cause said device to permit said parameters to be input by signals sent to said device.

42. The carrier according to claim 40 which is adapted to cause said processor to permit one set of parameters to be associated with a group of data content entities controlled by a party external to said device, and a different set, or different sets, of parameters controllable by a different party external to said device, or further external parties.

43. The carrier according to claim 40 which is adapted to cause said processor to permit a specific data content entity to have a plurality of parameters relating to it, and to permit different parties to set different parameters of the same data content entity.

44. The carrier according to claim 41 which is adapted to cause said processor to enable third party mediated control of the response of the NASD to user requests to store or access data content entities.

45. A programmed memory storing a program which when run on a processor of a computer memory network attached storage device having a processor, a non-volatile memory, and a library of signatures or fingerprints, is adapted to cause said storage device to:

evaluate data content of a data content entity either stored in said memory or received by said device for storage in said memory and to create a signature or fingerprint derived from said data content and capable of identifying said data content;

and to compare said created signature or fingerprint with reference signatures or fingerprints held in said library of signatures or fingerprints for establishing

whether said created signature or fingerprint matches a reference signature or fingerprint and for thereby establishing an identity of said data content; and

perform a predetermined act which is influenced by said identity of said data content.

46. The programmed memory according to claim 45 wherein said predetermined act includes communicating externally of said device information that is related to said identity of said data content.

47. The programmed memory according to claim 46 which causes said device to refer to a set of content-related parameters in determining what is to be said predetermined act.

48. The programmed memory according to claim 47 which is adapted to cause said device to permit said parameters to be input by signals sent to said device.

49. The programmed memory according to claim 47 which is adapted to cause said processor to permit one set of parameters to be associated with a group of data content entities controlled by a party external to said device, and a different set, or different sets, of parameters controllable by a different party external to said device, or further external parties.

50. The programmed memory according to claim 47 which is adapted to cause said processor to permit a specific data content entity to have a plurality of parameters relating to it, and to permit different parties to set different parameters of the same data content entity.

51. The programmed memory according to claim 48 which is adapted to cause said processor to enable third party mediated control of the response of the NASD to user requests to store or access data content entities.

52. A method of controlling access to a memory of a data storage unit, the method comprising using knowledge of content of data content entities stored in, or to be stored in, said memory and a knowledge of user identity, and acting dependent upon said knowledge of the content and the identity of the user, said act being causally connected with a communication to or from a third party different from the user.

53. A network comprising:

an attached storage device having a memory and having details of files accessible through said device, details of users entitled to access said device for at least one of read and write operations, and a set of rules specifying actions to be taken upon receipt of a request from allowable users to access files, said rules being dependent upon the identity of at least one of a user and content of the file concerned;

a network link for enabling said device to be connected to a third party on the network; and

a processor as part of said device configured to monitor access by users to files and to communicate with a network attached third party data that is user and/or file dependent and representative of user-data content access activity.

54. A device according to claim 1 further comprising a programmed set of rules for determining what is to be said action;

wherein said memory is adapted to store a plurality of data content entities having data content;

wherein content-related parameters are adapted to be available to said processor, said content-related parameters being associated with corresponding data content entities;

and wherein said set of rules is adapted to use those of said content-related parameters which relate to a selected data content entity for determining what is to be said consequential action when said selected data content is established as having a characteristic or derivative that matches a known characteristic or derivative.

55. A device according to claim 54 further including a telecommunications connector, and said processor is programmed for enabling a third party external of said device to set at least some of said content-related parameters.

56. A device according to claim 55 wherein said content-related parameters have an associated content-related parameter control authority and said processor is programmed to determine that said third party is authorised to control at least the, or those, of said content-related parameters that said third party sets prior to allowing said third party to set the parameter or parameters.

57. A device according to claim 54 further including a user-identity and wherein a data content entity access concordance is adapted to exist, said concordance being arranged for influencing which data record entities in said memory can be accessed by which users, said processor being programmed to use said user-identity and said data content entity access concordance for determining whether or not a user is granted access to a data content entity stored in said memory.

58. A device according to claim 44 further including a user identity for enabling said processor to identify a user who requests at least one of read and write access to said memory; and wherein said set of rules is adapted to use the user identity as a factor in determining what is to be said action.

59. A device according to claim 54 wherein said processor is arranged so (a) said characteristic of said selected data content is established as matching a known characteristic by processing said selected data content to produce a representative fingerprint or signature and (b) said representative fingerprint or signature is compared with a library of known fingerprints or signatures representative of known data content.

60. A method of providing at least one of read and write access to a data record entity stored in a computer readable memory of a network attachable data storage device having stored therein or accessible thereto:

(i) information correlating a plurality of data record entities stored in said memory and content-related characteristics adapted to identify an equivalent said data record entity; and

(ii) access authority parameters associated with said data record entities or said content-related characteristics; the method comprising:

accompanying requests by a user access authority for at least one of read and write access to data content entities, there being a relationship between user access authorities and access authority parameters to enable a user to access data record entities for which the user has authority for read and/or write access, evaluating a user's access authority indicia and an access authority parameter of a requested data content entity by using the network attachable storage device.

61. The method of claim 60 further including determining whether access is granted or not in response to the evaluating step.

62. A method according to claim 60 further including generating an invoice for accessing data content entities by using an assessment of the identity of said user and identities of data content entities accessed by said user.

63. A method of integrated storage of rights-controlled data content entities and billing for at least one of storage and use of said rights-controlled data content entities, said method comprising

(i) evaluating requests for at least one of storage and read requests for access to memory of said device by using a network attached storage device, and comparing identities of users making said requests with content-related indicators by using a network attached storage device, and

(ii) generating billing relating to user access request activity based upon user identity and content identity.

64. The method of claim 63, further including determining whether said requests are allowed.

65. A computer accessible data storage device comprising a data store and a processor,

said processor comprising reference data content characteristic means having or being adapted to obtain, reference data content characteristics representative of known data content, and content identifying means adapted to evaluate a selected data content against said reference characteristics from said reference characteristic means for determining whether a characteristic of said selected data content matches a said known data content characteristics;

and said processor being programmed to take a consequential action in response to said content identifying means establishing that a characteristic of said selected data content matches a known characteristic.

66. A Network Attached Storage Device having:

a machine readable computer memory for storing data content entities in the form of files having a data content that is the information content of the entity; and

a memory access controller having a control processor operable to evaluate selected said data content to establish whether there is a match between a content-identifier, indicia, fingerprint or signature of said selected data content and a reference content-identifier, indicia, fingerprint or signature;

said control processor being adapted to (a) cause a file received by said Device and requested to be stored in the Device to be stored in computer memory, (b) cause data content of said received file to be evaluated for determining whether said file should continue to be stored or not, and (c) cause said received file to be stored for access by users or not stored for access in response to evaluation of said received file data content.

67. A device according to claim 66 wherein http compatible functionality is supported by the processor.

68. A Network Attached Storage Device having:

a machine readable computer memory for storing data content entities in the form of files having a data content that is the information content of the entity; and

a memory access controller having a control processor operable to evaluate selected said data content to establish whether there is a match between a content-identifier, indicia, fingerprint or signature of said selected data content and a reference content-identifier, indicia, fingerprint or signature;

said control processor being adapted to (a) cause a file received by said Device and requested to be stored in the Device to be stored in computer memory, (b) cause data content of said received file to be evaluated to determine whether said file should continue to be stored or not, (c) cause said received file to be stored for access by users or not stored for access in response to evaluation of said received file data content, or (a') monitor third party access to data content stored upon said device and to bill an appropriate entity for accessing said data content.

69. In combination, a non-volatile memory for storing data content, and a control processor operable to take an action in response to a positive comparison between evaluated selected data content of the memory and a reference data content thereof.